CAMBRIDGE
UNIVERSITY PRESS

RESEARCH ARTICLE

Blockchain networks as constitutional and competitive polycentric orders

Eric Alston[1] (iD), Wilson Law[2] (iD), Ilia Murtazashvili[3*] (iD) and Martin Weiss[3] (iD)

[1]University of Colorado, Boulder, USA, [2]Baylor University, Waco, USA and [3]University of Pittsburgh, Pittsburgh, USA
*Corresponding author. Email: ilia.murtazashvili@pitt.edu

Abstract
Institutional economists have analyzed permissionless blockchains as a novel institutional building block for voluntary economic exchange and distributed governance, with their unique protocol features such as automated contract execution, high levels of network and process transparency, and uniquely distributed governance. But such institutional analysis needs to be complemented by polycentric analysis of how blockchains change. We characterize such change as resulting from internal sources and external sources. Internal sources include constitutional (protocol) design and collective-choice processes for updating protocols, which help coordinate network participants and users. External sources include competitive pressure from other cryptocurrency networks. By studying two leading networks, Bitcoin and Ethereum, we illustrate how conceptualizing blockchains as competing and constitutional polycentric enterprises clarifies their processes of change.

1. Introduction

Blockchains burst onto the scene with the introduction of the Bitcoin cryptocurrency in 2008. With Bitcoin enjoying a years-long meteoric price rise and Ethereum garnering attention from investors and users of network services, cryptocurrencies remain the most prominent application of permissionless (or public) blockchains today. Scholars, too, have devoted attention to these networks and their underlying technology. Many have highlighted permissionless blockchains' novel institutional features, including complete contracts, trustless transactions, nondiscretionary monetary rules, distribution of governance authority, high network transparency, and pseudonymity for users.

We argue that this conventional view is overly static and understates the extent to which these networks – much like large, complex organizations – and their protocols evolve in response to users' threat to exit and a polycentric set of internal and external governance forces. This relationship makes blockchain networks polycentric, in that they are subject to the social rules that emanate from multiple decision centers (Aligica and Tarko, 2012), social rules which include institutions articulated through the formal collective choice mechanisms of specific organizations, as well as norms emanating from the cultural groups that exist within and around these organizations (Alston *et al.*, 2018). Importantly, this 'entangled' or 'embedded' nature of organizational decision centers (including those of blockchain networks) means these decision centers are governed by the forces of competition (Alston, De Filippi *et al.*, 2021, Alston, Law, *et al.*, 2021), which makes these networks' governance a function of multiple decision centers characterized by their institutional frameworks and evolutionary competition among them.

The internal forces that define this rule-based governance include blockchain protocols, power concentrations, and collective-choice rules that meet the ongoing need to adjust network processes (and the underlying protocol) and resolve collective-choice dilemmas. The external governance forces are competitors' performance (partly resultant from their individual governance choices) and the set of public and private institutional authorities to which the networks are subject, the former category of which notably includes the legal and regulatory treatment of blockchain networks by state actors (Alston, forthcoming). Much of these internal and external forces (and their resultant rules, or constraints on the collective choice process of a given blockchain network) can be explained by: (i) public choice theories of constitutional political economy; and (ii) quality and feature competition in the field of industrial organization. Using these theories, we compare several major permissionless blockchain networks – but focusing on Bitcoin and Ethereum – to illustrate why a descriptive polycentric theory of blockchain better explains observed outcomes than the conventional view. More specifically, we show how blockchains evolve in ways that a complete-contract or trustless view cannot explain.

To reach these conclusions, we first survey the existing literature on the beneficial institutional characteristics of cryptocurrencies, and then we provide a brief overview of how permissionless-blockchain technology supports cryptocurrency networks. We then characterize blockchain networks as subject to internal forces of constitutional political economy arising from the need to update their protocols in light of unanticipated circumstances or changing network needs. Next, we explain how blockchain networks are also subject to external governance forces, among which competition stands tall, which directly indicates the explanatory benefits of competitive firms as a lens through which to understand these networks' comparative performance over time.

2. Institutional analysis of blockchain networks' benefits

Blockchain has been described as replacing law by the rule of code (De Filippi and Wright, 2018), creating a new and digital form of trust (Werbach, 2018), and providing a novel governance structure that does not require trusted third parties to process transactions (Allen *et al.*, 2019; Davidson *et al.*, 2018; Frolov, 2021). These trustless features of blockchain have received considerable attention among proponents of cryptocurrencies and scholars of institutional design alike. One of our contributions is to add more institutional detail to these studies, which view blockchain networks as an alternative to firms, relational contracting, and governments as a new building block of a capitalist economy. We also aim to clarify the dynamic and polycentric aspects of blockchain governance, moving the analysis closer to Williamson's (1996) complexity view of the firm. Relatedly, Frolov (2021) finds that blockchain institutions are hybrids of conflicting institutional logics – regulatory and algorithmic law, public and private systems – and contracting logics. Our polycentric view integrates and adds to the insights from these perspectives.

For many advocates of cryptocurrencies, their most important feature is that they are free from the interference of a single powerful group of people. As Cowen (2019) explains, opportunities for choosing them means opportunities for entrepreneurs (broadly defined) to alienate their authority to achieve self-governance in the face of concentrations of economic power (such as corporations) and government power (such as centralized banking). Cryptocurrencies' blockchain protocols also provide a constitutional structure that defines user and participant citizenship on the network (which can be essentially open to all), determines exit costs and enumerates the participants' powers (Alston, 2020).

Another perceived benefit of permissionless cryptocurrencies, and blockchain technology, more generally, is that they do not rely on trusted intermediaries to process transactions. In a modern economy, most economic activities depend on a few intermediaries to process and validate transactions, which makes these intermediaries very powerful. Those concerned about such influence point to bargaining power, political influence, and the weaknesses associated with having a single point of failure (Berg, 2021). Most cryptocurrencies also offer their users identity protection, which makes the users effectively pseudonymous and thus transact more privately. They also enable people to transact seamlessly and inexpensively across national borders. For these reasons, cryptocurrencies inspire many to

envision a future free of government intervention. People will be able to transact with smart contracts, or even real property, free from the prying eyes of the government and the intermediation fees of banks, credit card companies, and marketers. We contend that some of these visions are likely to remain aspirational, as they rest on a misunderstanding of what can be governed purely digitally (Alston, De Filippi *et al*., 2021, Alston, Law, *et al*., 2021). Blockchain technology faces many challenges in implementation, and various market and governance forces are at work defining the margins on which blockchain networks will facilitate transactions, a specific case of the need for additional governance layers in large impersonal digital networks that has been identified elsewhere (Harris 2018).

Bitcoin's issuance process is transparent and free from government or central bank control, so many scholars have studied the benefits of the monetary rules underlying it and other major cryptocurrencies (Weber, 2016). In many economies, monetary rules are unreliable (Boettke *et al*., 2021). Even the supply of US dollars, considered one of the world's most reliable currencies by institutional and sovereign investors, is managed by the Federal Reserve through a complex and at times highly politicized set of policy tools.[1] For those skeptical of the Federal Reserve's ability to maintain a stable currency (Salter and Tarko, 2017), Bitcoin's fixed money supply rule is attractive. However, the value of Bitcoin and other cryptocurrencies relative to the dollar has proven highly volatile (White, 2015), which suggests that issuance rules are likely to be a source of ongoing competitive differentiation among cryptocurrency networks, a point we consider in detail later in our analysis.

De Filippi and Loveluck (2016) identify two distinct governance mechanisms in Bitcoin – the infrastructure governed by code and the management of the infrastructure by a small group of core developers. DuPont (2017) recognizes that blockchain systems require governance beyond the agreed-upon protocols, an idea we extend by considering additional forms of external governance, including competitive aspects of blockchain, as suggested by Alston (2020). Berg and Berg (2020) consider exit and voice in blockchain, an idea we extend by considering blockchain's change processes beyond those defined by forking, including through competition from other blockchain networks.

Given how competitive the cryptocurrency space has been thanks to low entry costs, distinct permissionless blockchain networks have emerged competing for users and network participants. In light of this competition, Garriga *et al*. (2020) classify popular blockchain systems according to experts' assessments of their cost, consistency, functionality, performance, security, decentralization, and privacy. Halaburda and Sarvary (2016) review the consensus algorithms and monetary rules, among other features, of 10 major cryptocurrencies. As with legal systems, constitutions, or economies, blockchain networks' features are highly tractable to comparative analysis, which we expand through the lens of competitive industrial organization.

Because blockchain helps mitigate certain types of counterparty risks, innovative applications such as smart contracts (Howell and Potgieter, 2021), registration of real property (Arruñada, 2018), and decentralized autonomous organizations (DAOs) (Wright and De Filippi, 2015) have been heralded, although these applications face many structural challenges (Arruñada, 2018). Blockchain-technology advocates also promote the idea that a network built on blockchain can govern itself through its transparent protocol. These features arguably make blockchain an innovation commons – an institution that governs the cooperative pooling of innovation resources and facilitates entrepreneurial discovery (Potts, 2018).

These features of blockchain networks show how the networks' unique institutional characteristics distinguish their governance from the traditional governance provided by governments and firms. We now discuss the core attributes of permissionless blockchains from an institutional perspective in order to subsequently analyze – with the aid of theories of public choice and industrial competition – how these attributes derive from nested governance forces.

---

[1]The exercise of these policy tools is frequently influenced by political or social exigencies to the point that monetary supply becomes inextricable from fiscal policy, which is another defect that advocates of permissionless-blockchain networks point to when defending the more rigid or even deflationary monetary rules embedded in cryptocurrency protocols.

3. An institutional overview of permissionless blockchains

Cryptocurrencies are the fruit of networks that maintain a distributed ledger surrounding these units of account, individual network identities, and interactions between these identities and the units of account. The day-to-day processing of these interactions is governed by specific algorithmic protocols. For most cryptocurrencies, the structure of the network created by the blockchain protocol results in each network member keeping a copy of the digital ledger of transactions of the entire system and users transacting with one another directly without relying on a central third party to validate and process proposed transactions. The systems are usually run on open-source software so that the operation is transparent and easily auditable, and replicable by interested parties.

Blockchain networks vary depending on how users and participants can join them. A permissioned blockchain has a central organization to determine the characteristics that qualify one to participate in or use the network. In contrast, permissionless-blockchain applications allow anyone to freely participate in network processes or use the services of the network surrounding its underlying unit of account.[2] Bitcoin was the first permissionless-blockchain-supported cryptocurrency, is the most well-known permissionless-blockchain application, and commands a majority of the cryptocurrency market's capitalization. On the Bitcoin network, and in the many similarly structured cryptocurrencies, a user transacts with other users through an address (pseudonym) on the network. To send the network's digital units of account to another user, a sender broadcasts the proposed transaction to the network with a transaction fee attached. Miners compete to process the transactions to earn a fee and a block reward from the system. Each miner collects a set of proposed transactions into a block and verifies whether those making requests have valid ownership claims (i.e. sufficient funds in their account). Miners need to solve a cryptographic puzzle before they can attach the new block to the public chain. The distributed ledger maintained jointly by all network participants, therefore, comprises a chain of blocks of transactional data, where each block links to the preceding one: hence the name blockchain. The first miner who solves the puzzle earns the right to add their new block with its accompanying block and fee rewards. Winners of the race are effectively randomly selected, which ensures helps ensure miners have incentives to process transactions in good faith.[3]

What is unique about cryptocurrencies is that the network structure is distributed and transparent. It is transparent in that the full history of the blockchain is publicly available to network users, and distributed in that the governance authority for processing and validating transactions resides with some probability with all network participants (Luther and Stein Smith, 2020). All of the cryptocurrencies' protocols are embedded in open-source programs that also make the code-based process transparent itself to any interested party. The result is a peer-to-peer electronic cash system that does not rely on trusted third parties to process payments, as envisioned by Nakamoto (2008). Any user can leave and rejoin the network at will, and no central authority determines who can perform network functions. The government, therefore, has a limited role in determining a cryptocurrency's value, which, unlike modern fiat currencies' value, is determined primarily by users' individual valuations (Catalini and Gans, 2016).

Cryptocurrencies thus enable any knowledgeable person with access to the technology to become a potential decision-maker on the network. Developers can change the structure of the network significantly. If a developer proposes a protocol update that is supported by a sufficiently large subset of miners but opposed by an equally large or larger subset, a protocol update can create a new blockchain network through a hard fork (creating two blockchain networks whose identical histories up to the

---

[2]Participation in network processes includes processing and validating transactions, as well as potentially participating in the ongoing processes of governance surrounding protocol updates. Some networks, such as the upcoming Ethereum 2.0 network, do not have a structure that is open for anyone to *participate* in network processes, even though the network will be open for anyone to *use*.

[3]Technically, the selection probability is proportional to the computational power of the miner relative to the computational power of all miners. As long as no miner has overwhelmingly large computational power, no one can consistently win the race and thus be able to tamper with the blockchain without being noticed.

time of the update are independent thereafter) or a soft fork (such that the new protocol remains compatible with existing software). Miners do not make decisions through a centralized hierarchy as in a firm but through a distributed process of decision-making that gives them collective influence over the network. The rule determining whether blocks are successfully added to the blockchain and whether protocol updates are accepted is known as the consensus mechanism or consensus algorithm. The specific consensus mechanism used on the major permissionless-blockchain networks[4] accords network participants an unparalleled level of participation and governance authority – more akin to what members of a constitutionally constrained public entity enjoy than what members of most private organizations and citizens in centralized monetary systems have (Alston, 2020).[5] The networks are governed by the aggregation of individual network participants' decisions. Despite their unique features compared to traditional forms of network (organizational) governance, blockchain networks are susceptible to a concentration of power due to protocol-design choices made in pursuit of specific network features, for the proof-of-work (PoW) consensus mechanism directly preferences massive concentrations of graphical processing power. In conjunction with local variation in the cost of electricity and internet access, this defines an equilibrium level of processing power at which resolution of the underlying cryptographic hash function is economically competitive. This results in both an internal political economy, as well as an institutional (protocol) design margin on which new entrants can compete with incumbents, both governance forces that we treat in detail subsequently.

Open-source cryptocurrencies' operational rules and processes are transparent in that any interested party can scrutinize them. For example, with Bitcoin, the money supply and its growth rate are common knowledge. One can also directly inspect the blockchain to count the exact number of tokens on the network.[6] The money supply follows a predefined process in which miners receive new tokens as rewards for adding new blocks to the blockchain. In 2009, when Bitcoin first started, the block reward was 50 Bitcoin. The protocol specifies that after every 210,000 blocks, the reward is halved. Given that miners create a block roughly every 10 minutes, the reward is halved approximately every 4 years. The design results in the mathematical certainty that 21 million Bitcoin will be created by the time rewards fall to zero around 2140 (King *et al.*, 2013).

Commentators generally see blockchain networks' institutional design as innovative because of the way it distributes authority, provides an immutable and transparent record, and incentivizes users to participate without the benefit of traditional sources of incentives such as residual claimancy for firm managers. But this view only scratches the surface, for protocol-design choices result in a constitutional political economy unique to each blockchain network, which is also subject to external governance forces. We better define the contours of these types of governance in the subsequent two sections, using the theories of constitutional political economy and industrial organization, respectively.

4. Blockchains' constitutional political economy

Permissionless-blockchain networks are governed by a protocol, which has been described as much like any constitutive organizational choice (Alston, 2020; Cowen, 2019; Rajagopalan, 2018). If cryptocurrency networks could go without protocol change forever, they would be free of human intervention. But even though the technology is innovative in combining several established approaches in computer science, the networks are still complex human organizations that cannot anticipate all possible challenges (for example, flaws in the software, or unanticipated events) after they go live. Even though cryptocurrencies are designed to be governed autonomously, in practice they require

---

[4]The specific way in which these blockchain networks reach consensus is known as proof of work.

[5]The level of necessary participation in governance is minimal on these networks, but in relative terms, they are a network that enables voice – a more general feature of blockchain (Berg and Berg 2020).

[6]It is not known how many tokens are still active because when a user loses the password to a token, that token is lost forever. Theoretically, the number of tokens might gradually decline after the minting process stops. The cryptocurrency-data firm Chainalysis in its 2020 *Crypto Crime Report* that 20 percent of all Bitcoin have not been moved for five or more years. It considered these coins to be lost.

continuous updates and maintenance. They face challenges resembling those of most organizations. A group of software developers continually maintains the software. The process of proposing, choosing, and adopting changes to the software creates distinct interest groups of developers and stakeholders negotiating over the future direction of the networks.[7] The negotiation entails extensive debates before the groups reach a consensus, if at all. A few recent high-profile events that triggered software changes highlight the importance of collective decisions in the governance of the networks.

4.1 Protocol change as constitutional change

Consider first a well-publicized debate in 2010 within the Bitcoin community about the size of a block, which was then fixed at one megabyte.[8] The block size determines how many transactions can be included in a new block. As Bitcoin's popularity grew, users became concerned that the system might not be able to handle the increasing number of transactions in a timely fashion.[9] If transaction demands were to increase past a certain point continuously, some proposed transactions might never get processed because the transacting parties would be outbid by other users who are consistently willing to pay higher fees for their own transactions. This would in theory drive users to competing networks, although the theoretical effects on miner rewards from transaction fees as a function of block size is ambiguous. Some users proposed an increase in the block size, but the proposal came with trade-offs including surrounding the effect on transaction fees.[10] Ultimately, the disagreement over these trade-offs was sufficiently intense among network participants that a hard fork of the Bitcoin network occurred, creating a new blockchain network, with an associated unit of account, Bitcoin Cash (BCH).

The first concern was the security of the network. Increasing the block size would increase the size of the blockchain (the complete ledger), which would require more storage space and network bandwidth to download and upload it. It would also require more computational resources to validate all the transactions. As a blockchain is maintained (and monitored) by users who voluntarily participate in the network, fewer users would monitor and validate the transactions if it became increasingly costly. Larger blocks are also more resource-intensive to process, but miners would receive the same reward as before for a new block, unless transaction fees increased to compensate them for the added cost. The increased costs would discourage miners with fewer resources and potentially concentrate mining power among a few well-endowed miners. This concentration of power would make the network more vulnerable to malicious attacks (for example, users tampering with the blockchain to spend Bitcoin twice) because the system depends on the assumption that a large percentage of the miners are honest.[11] As the mining pool would shrink, it would grow harder to ensure the integrity of the miners. Moreover, smaller blocks arguably make transaction slots more valuable. Users might bid up transaction fees to have their transactions processed faster. If the fees were not so high that they drive users to competing networks, miners could in theory earn more with smaller blocks.

Thus, a seemingly technical choice had significant redistributive implications, as it involved parties with conflicting interests who had made costly investments based upon the status quo protocol and

---

[7]Indeed, in the early Bitcoin community, members recognized the importance of coordinating users and did so (Luther 2019).

[8]See De Filippi and Loveluck (2016) for more details.

[9]To put it in context, Narayanan et al. (2016) estimated that, at the time of writing, Bitcoin could process about seven transactions per second. In contrast, major credit card networks such as Visa are reported to handle about two thousand transactions per second on average around the world. At peak times, they can handle ten thousand transactions per second.

[10]Accompanying the discussion was a proposal to change the software architecture to store the transactions more efficiently. For more details, see 'Segregated Witness (Consensus layer)' in Bitcoin Improvement Proposal BIP141.

[11]The security of blockchain is an area that has unsurprisingly been extensively researched and discussed (see, for example, Li et al. 2020).

their expectations about likely protocol changes.[12] Just as improvements in the face of changed cir-cumstances (such as the drastically increased demand for transacting in Bitcoin) require protocol updates with political-economic consequences, reversing undesirable outcomes also demands network responses with political-economic effects, as illustrated by the following case.

In 2016, a small blockchain company, Slock.it, launched a crowdsourced venture fund, the DAO, on the Ethereum platform.[13] It allowed cryptocurrency investors to fund and manage new businesses with Ethereum's digital currency, Ether. Within weeks of the launch, a hacker found a software loop-hole that allowed them to steal a quarter of the pooled funds, worth millions of dollars at the time. Since the system is autonomous and decentralized, there was no easy way to stop the outflow imme-diately, although the stolen funds were held in an escape pod where the hacker could not yet dispose of them at their discretion.[14] This gave the Ethereum community a fixed period to debate how to respond to the theft. Ethereum's founder, Vitalik Buterin, and other key leaders proposed to reverse the trans-actions to return the funds to the investors. Other network participants objected based on the principle that network processes, and hence sealed blocks, should be immutable. They were concerned about setting a precedent that would allow the community to alter the blockchain for other purposes. The two sides could not reach a consensus, and the impasse led the Ethereum network to split into two systems. The majority of users followed Buterin and the other prominent figures, and others broke off to create Ethereum Classic, a new chain where the stolen Ether (now called ETC or Ether Classic) lives on.

This incident highlights the importance of governance by key players in the blockchain system, even though it was designed to be autonomous and has no centralized governing authority; a suffi-ciently malicious attack caused two fundamental principles to come into direct conflict (Alston, 2020). The network participants who thought bad actors should be publicly punished went with the Ethereum network, while those who thought immutability of code should triumph went with the original blockchain. The incident highlights that protocols cannot amend themselves and adjudi-cate unanticipated conflicts, which means the burden of governance falls on humans and usually only a few humans.[15]

4.2 Concentrated influence in protocol updates

How do cryptocurrency networks react to challenges? How are decisions made and proposals imple-mented? Who are the major decision-makers, and how much power do they have? To answer these questions, we need to understand how open-source software operates in a decentralized network.

The two largest cryptocurrencies, Bitcoin and Ethereum, operate on open-source software plat-forms. An open-source software program's source code is publicly available, allowing anyone to study it and run the program. Bitcoin and Ethereum both have a process to change their protocols – namely, the Bitcoin Improvement Proposal and Ethereum Improvement Proposal. In these pro-cesses, a proposal typically begins with informal discussions within the community, such as GitHub for Ethereum.[16] After the idea is refined by the community and receives sufficient support,

---

[12]Ironically, despite concern as to concentrations of mining power resultant from larger block size, processing power on the Bitcoin network is highly concentrated, as it also is on the Lightning Network, a subsidiary payment network on the Bitcoin blockchain (Bartolucci et al., 2020; Lin et al., 2020).

[13]Dupont (2017) provides more details to illustrate these aspects of governance.

[14]One of the challenging incentive problems associated with semi-automated allocation of funds to investment projects predicted to yield a future return in excess of the initial investment surrounds depletion of the entire fund during especially high points, which led to the DAO's protocol involving a holding period before funds were released to a user's wallet. The ETH the hacker obtained was withdrawn from the DAO itself, but had not yet been transferred to the hacker's private wallet – the unique and individual addresses apart from the DAO yet separate from users' wallets where a withdrawal was held came be to known vernacularly as 'escape pods'.

[15]For additional cases, see De Filippi and Loveluck (2016).

[16]See for example https://eips.ethereum.org/, https://github.com/ethereum/EIPs, https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1.md.
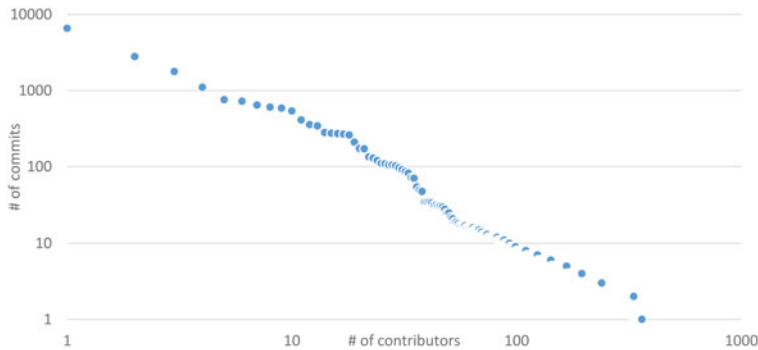
Figure 1. Distribution of bitcoin commits.

a developer submits a draft proposal. A code change requires intimate knowledge of the software, so it is not surprising that most proposals come from a small group of developers. Figure 1 presents the number of 'commits' (accepted code changes) on a log scale as a function of the number of Bitcoin contributors. A power-law distribution indicates that a few contributors have made many code changes, while many contributors have made very few changes. As in most open-source software, software developers do not receive payment for their time and effort, at least not directly.[17] Most developers contribute out of the desire to provide a public good. In cryptocurrencies, early developers who own many tokens have an added incentive to contribute: if the currencies become widely accepted, their holdings are likely to rise in value.[18]

Although a small number of core developers tend to dominate protocol updates, their power is not unchecked. Miners ultimately process the transactions and create the blocks. On a distributed network, no one can force them to adopt the new software or changes. If they do not adopt the protocol changes, the blockchain will remain the same. Likewise, no one can force users to adopt or upgrade. But the ability to exchange tokens requires compatibility between users and miners. The accompanying network effect incentivizes users to coordinate on the same version of the blockchain. Similarly, to earn block rewards and fees, miners adopt the version that is compatible with what users are using. Similar network effects apply in the cases of merchants, exchanges, wallets, and other auxiliary service providers. As a result, even though software developers, users, miners, and service providers make strategically independent decisions as in a non-cooperative game, the outcome is effectively an equilibrium play of a coordination game. Therefore, when a network is confronted with a challenge, solving it requires the consensus of a sufficient number of stakeholders. If enough miners do not adopt the new software, then any changes are moot. The decision process, therefore, requires serious consensus-building among stakeholders because adopting code changes ultimately rests on what network participants do.[19] This consensus requirement is only heightened given the extent to which permissionless blockchain-network participants hold rule by code as a governance principle (Alston, De Filippi *et al.*, 2021, Alston, Law, *et al.*, 2021).

But what happens when consensus cannot be reached on new proposals? In the easy case in which a change in the software can be made backward compatible, all users and miners can adopt it without

---

[17]For more on the motivations of contributors in the open-source community, see, for example, Newman et al. (2012). Bosu et al. (2019) examine the motivations of the developers in the Bitcoin community. They find that the motivations of participants vary but include intrinsic motivation, external rewards, ideology, community recognition, and learning.

[18]Well-known cryptocurrency developers such as 'Satoshi Nakamoto', Gavin Andresen, and Vitalik Buterin all reported that they owned a substantial amount of cryptocurrency.

[19]There is clearly evident in this interview with some of the core Bitcoin developers: https://www.youtube.com/watch?v=MGiv-OuIA5I. The adoption of a soft fork is also discussed here: https://bitcoinmagazine.com/articles/bip-8-bip-9-or-modern-soft-fork-activation-how-bitcoin-could-upgrade-next.

disrupting the network. Or multiple versions of the software that follow the same protocols can coexist and still allow the users to exchange tokens.[20] When a change in software or protocol cannot be made backward compatible, miners, though autonomous agents, act collectively with respect to the drafting, consideration and implementation of protocol updates, though the change need not be unanimously adopted. If enough miners or users adopt a change, then miners who do not adopt it are left behind and lose the opportunity to earn fees from mining (and to easily transact with their prior mining rewards) and users who do not adopt the change lose the exchange network (and their units of an account located thereupon). Miners and users can choose to comply, or they can branch off in a hard fork. If a sufficient number of users and miners decide to branch off, and the network is large enough for them to coordinate on a new focal point, a new network is formed, as was the case with BCH and ETC. The new network can create (or move to) a different market, compete with the incumbent network in the same market, or position itself somewhere in between. The threat of a new competitor is a strong governing force that restrains the dominant network and is, therefore, the subject of our next discussion.

5. External competitive governance of blockchain networks

Because of cryptocurrency networks' nature in facilitating the exchange of economic value, network participants and users are subject to a variety of laws and regulations concerning property, contracts, taxes, and securities. While these laws and regulations are undeniably an important source of external governance pressure, a comprehensive summary of the public and private institutions governing blockchain networks is beyond the scope of this analysis.[21] Just as importantly as that source of pressure, though, is that private networks that reliably and immutably process digital units of account are providing services to a user base that can easily use competitors' services as substitutes for or complements to a given network's services. Competition, therefore, constitutes a critical source of external governance. New software platforms often emerge when developers see room for improvement. Software platforms compete for users and, as a result, indirectly govern one another; network users' and participants' voices and the threat of exit apply as in other governance contexts (Hirschman 1970).

5.1 Competitive governance of cryptocurrency networks in theory

Some scholars (for example, Lee *et al.*, 2020) consider the governance of blockchain as a political process in which users vote with their feet to determine which fork survives. However, a crucial distinction between electoral and market processes is that all users consume the majority-chosen product after an election, but in a market environment, users consume the product of their choice. One way to understand the competitive dynamics among permissionless cryptocurrencies (and their close substitutes) is to think of firms as competing in the market for similar or identical user bases. Therefore, a natural choice of framework for studying the competitive governance of cryptocurrencies is that of product differentiation and quality competition in the field of industrial organization. In the terminology of industrial organization, competition can manifest in the vertical (quality) dimension and the horizontal (feature differentiation) dimension. In the context of cryptocurrency, the distinction between

---

[20]Lopp (2020) reports that about 96 percent of the Bitcoin nodes implement Bitcoin Core; the rest of the nodes run on a dozen or so distinct implementations.

[21]Related research considers the question of public and private institutional governance of blockchain networks from a legal perspective (Alston, forthcoming; Alston, De Filippi et al., 2021, Alston, Law et al., 2021). For example, most users eventually rely on exchanges to convert their digital holdings to fiat currencies. Gains made from holding cryptocurrencies tend to be subject to taxation. User identities might need to be reported by the exchanges subject to money laundering regulations. If users do not receive the payment promised or the goods or services they paid for, they can potentially resort to legal actions to enforce their contracts. Given the innovative nature of blockchain networks, they have required, and will likely continue to require, ongoing definition in relation to a given nation's legal regime, such that law and regulation stand as a major external governance force that will shape a given network's development in the years to come.

quality and feature differentiation is not always easy to discern. However, it offers a useful framework to evaluate each cryptocurrency's features from network participants' and users' perspectives.

To understand how competition influences governance in this context, we need to review the economic forces at work for each type of player on cryptocurrency networks. From a user's perspective, the monetary cost to move to a different platform is relatively low. Like citizens voting with their feet to influence political decisions (Somin, 2020), the threat of cryptocurrency users exiting to a better-governed network induces platforms to protect users' interests. Because the value of a cryptocurrency is mostly a function of the size of the currency's user base, platform developers, miners, and community members who own large stakes in the currency have substantial incentives to expand the user base by promoting users' interests. However, large networks have more leeway than smaller ones in responding to users' demands because users enjoy more opportunities to exchange with merchants and users. The network effect, or positive externality, creates a barrier for other platforms seeking to lure users even when a given network is no longer the best option (Katz and Shapiro 1985). Currently, the cryptocurrency market is dominated (in terms of market capitalization) by Bitcoin (42.7%) and Ethereum (19.6%).[22] This domination suggests that most users prefer the benefit of a large network than the numerous differentiating features of competing cryptocurrency networks.

Finance scholars have considered the threat of exit as an instrument of governance through studying whether the threat of shareholders divesting their shares constrains firm governance. Increasing market liquidity (a proxy for ease of exit in publicly traded firms) is linked to increasing participation in governance by activist and passive shareholders: activists acquire a stake in the firms whose governance they actively engage in, while passive shareholders use the threat of exit to induce better governance (Edmans *et al.*, 2013). This split between two classes of stakeholders with the ability to exit a given cryptocurrency network corresponds directly to the difference in influence between cryptocurrency networks' participants and users. While key stakeholders vote on updates to the governance structure of the network and facilitate ongoing network processes, users can only influence governance by exiting the cryptocurrency network.

The network effect attracts miners as well. Increased adoption pushes up the exchange rates of cryptocurrencies and raises the value of block rewards. Higher rewards attract more miners and intensify the competition, which results in network-specific investments in equipment. This expensive equipment is designed for specific consensus algorithms, which may not be compatible with new cryptocurrencies with alternative algorithms, making it harder for miners to switch networks. The vested interest creates strong incentives for miners to preserve protocols that benefit them, although these protocol-design choices depend on the extent to which one network's protocol provides value to network users compared with competing networks' protocols.

In sum, competition makes networks sensitive not only to the demands of users but also to those of the collaborators (for example, developers, miners, and exchanges). From an institutional-design perspective, cryptocurrency networks are also like cooperatives managed by small numbers of influential leaders whose decisions ideally benefit customers (users) (Bosu *et al.*, 2019). Cryptocurrencies' core developers and major investors are instrumental in shaping a cryptocurrency because of their deeply held (often ideological) beliefs in the value proposition of their currency and potentially because of their substantial ownership of tokens.

To extend the analogy, a PoW blockchain network is like a worker-owned cooperative. Miners are like part owners in that they dedicate costly asset-specific investment capital to the production process they jointly engage in. They contribute costly capital in exchange for future rewards directly tied to the ongoing quality of the network's output. They have periodic (and typically decentralized) input into governance decisions. As we have stressed, though, the day-to-day output of the blockchain networks requires effectively no executive decision-making by those managing or using the network. Indeed, the touted benefits of blockchain are closely tied to the automatic way in which network processes are executed; human labor has been substituted by protocol-based production. But this separation of

---

[22]Market capitalization as of November 2021, on CoinMarketCap.com.

executive function from any concentrated residual benefits from the network's activity can in theory lead to a tragedy of the anti-commons if network participants' existing stakes in the network (and related exit costs) are insufficiently high to induce beneficial governance outcomes by incentivizing network participants to expend costly effort on governance.

In summary, cryptocurrencies are still on many important margins a nascent and rapidly evolving asset class, in large part because of changes to the underlying structure and purpose of blockchain protocols and the networks they support. Since most digital currencies are highly substitutable, market forces should in theory favor concentrated networks. Network effects clearly play a salient role because two cryptocurrencies represent over 60% of the market capitalization. Yet as of November 2021, there are 13,669 cryptocurrencies trading (according to CoinMarketCap.com), the fruit of a process that has been likened to the Cambrian explosion (Halaburda and Sarvary, 2016; Sokolin and Low, 2020). Competition among cryptocurrencies influences governance and protocol-design choices in the cases we detail in the subsequent subsection, which highlights the value of using the concepts of industrial organization to understand outcomes on blockchain networks. Since the switching costs for users are still relatively low, the threat from entrants is credible – a fact that facilitates comparative analysis.

5.2 Competitive governance of cryptocurrency networks in practice

The ongoing obstacles to large-scale adoption for any given cryptocurrency network also present opportunities for competing networks hoping to capture existing networks' market share or convince new user bases of the value of privately issued digital currencies through offering more efficient protocol design. Take Bitcoin. The network creates a new block roughly every 10 minutes, and merchants and exchanges usually wait for six or more blocks to be created (sixty-plus minutes) before confirming a transaction (Bonneau, 2015)[23]. This might be relatively fast for a cross-border money transfer, but it is nowhere near fast enough for use at checkout lines of grocery stores or coffee shops. Moreover, the PoW contest is considered by many to waste energy and also to concentrate mining power. Network critics argue that this concentration of power jeopardizes the security of the Bitcoin network. An additional issue is that the network design does not protect users' privacy to the extent desired by some, as founders of online drug markets have found to their chagrin. Economically, wide fluctuations of the exchange rate against fiat currencies weaken Bitcoin's use as a payment network and even as a store of value, given how common unpredictable precipitous declines in value are (alongside the major price increases that more naturally command headlines).

These are only a subset of the challenges that Bitcoin is facing; others include security and ease-of-use concerns. Given the opportunities for improvement and product differentiation that this subset of challenges (coupled with low entry costs and substantial investor interest) presents, it is not difficult to understand the explosion of competing cryptocurrencies. In addition to thousands of other cryptocurrencies in the space, Bitcoin also faces competition from traditional players such as state-issued currencies, incumbent payment networks (for example, Visa and MasterCard), and commodities (for example, gold and real estate).

Another major area of development among competing permissionless cryptocurrencies is the consensus algorithm, or the method of determining which miner can create a new block. The race to solve a cryptographic puzzle described previously is referred to as the PoW contest, which is effectively an all-pay auction or a Tullock contest (Halaburda *et al.*, 2020). Miners are engaged in a computational-power arms race because the probability of winning is proportional to the power they expend. To have a reliable chance of winning rewards, miners and mining pools increasingly invest in application-specific integrated circuit (ASIC) machines, which are custom-built machines that solve cryptographic puzzles specific to individual cryptocurrencies. The high cost of capital investment pushes out small, independent miners, resulting in the concentration of mining power, which some argue jeopardizes

---

[23]For a more contemporaneous estimate, due to the reality that transaction confirmation times vary widely as a function of network demand, see 'Bitcoin Average Confirmation Time' at https://ycharts.com/indicators/bitcoin_average_confirmation_time

network security. Another side effect of the PoW contest is that it is extremely energy-intensive (De Vries, 2018). An alternative, proof of stake (PoS), has been developed to alleviate the deadweight loss of the PoW race. Instead of randomly selecting validators of blocks proportional to their processing power, PoS randomly selects validators proportional to the sizes of the stake miners can demonstrate that they have set aside to display the alignment of their incentives with those of the network as a whole. This process bypasses the wasteful arms race but is not without its own trade-offs and implementation challenges. PoS is being implemented for the Ethereum network, with a test PoS chain mirroring the existing PoW blockchain.[24]

As for transaction processing, most non-Bitcoin cryptocurrencies (or altcoins) offer a faster transaction time than Bitcoin. Some offer more accessible mining algorithms by using alternative consensus rules. Litecoin, for example, uses a newer PoW algorithm (called scrypt) that requires less computation power so that miners with standard personal computers can participate.[25] These protocol design choices are intended to democratize the mining process and lower the total cost of running the network.[26]

Anti-inflationary protocol design is central to Bitcoin. The choice of a firm upper limit on the number of Bitcoin in circulation creates scarcity. But even without speculative activities and uncertainty about Bitcoin's future, the fixed money supply could still generate price volatility and deflationary pressure. Partly in response to the ongoing price volatility, Tether (alongside other currencies known as stable coins) offers a digital currency pegged to the US dollar by holding traditional currency reserves. Other cryptocurrencies supply a higher but still fixed amount of tokens, which alleviates the short-term scarcity problem but arguably does not address the fundamental challenge of a fixed money supply (Halaburda and Sarvary, 2016). Unsurprisingly, other cryptocurrencies, including Ether, do not have a fixed supply; they instead follow a variety of more discretionary monetary rules. In Ether's case, the network is committed to a standard of 'minimum necessary issuance.'[27]

In the feature space, many cryptocurrencies are differentiating themselves from Bitcoin and each other. Ethereum provides a rich programming environment to support smart contracts and DAOs. Ripple positions itself as a permissioned intermediary by offering to exchange currency for financial institutions across international borders. Monero focuses on privacy by making transactions on the blockchain nearly impossible to track or trace. Other cryptocurrency features are difficult to classify. For example, Dogecoin has an unlimited money supply and is designed for small transactions (such as digital tipping). Tezos tries to tackle the problem of splitting networks (hard forks) by having 'stakeholders govern upgrades to the core protocol, including upgrades to the amendment process itself.'[28] If it accomplishes its stated goal, the feature can be both a quality enhancement and a new governance feature.

Table 1 compares some of the leading blockchain systems (measured by market capitalization) in comparison with Bitcoin. The table illustrates the kinds of differentiation among systems. From this table, we can see the wealth of innovation within the blockchain ecosystem. The evolution of these markets has critical implications for the networks' governance.

The long-established industrial-organization theory indicates how competitors can engage in product differentiation in quality and in features. The BCH network, forked directly from the Bitcoin blockchain, provides a clear example of quality differentiation – faster transaction times facilitated by larger block sizes – while keeping other network features essentially identical, including the transaction history leading up to the time of the fork itself. The Ethereum network's white paper (Buterin, 2014) directly cites the Bitcoin network as inspiration but proceeds to detail how a programming layer can facilitate wider variety and greater complexity of transactional processes – a clear differentiation in

---

[24]https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ https://ethos.dev/beacon-chain/

[25]If Litecoin becomes valuable enough, miners will likely invest in more expensive specialized equipment, and so it has not solved the fundamental problem that confronts Bitcoin.

[26]https://litecoin.org

[27]https://docs.ethhub.io/ethereum-basics/monetary-policy/.

[28]See https://tezos.com/get-started.

Table 1. Notable blockchains

Cryptocurrency network (and consensus process)	Description	Differentiation
Bitcoin (PoW)[a]	The original permissionless-blockchain cryptocurrency network using a processor-intensive consensus mechanism	Relative to other networks, Bitcoin tends to be less prone to change because many network participants view immutability as a core design principle
Bitcoin Cash (PoW)	Bitcoin Cash forked from the Bitcoin blockchain after increasing the block size from 1 to 32 MB	Bitcoin Cash created a payment system with faster transaction speeds to improve scalability
Litecoin (PoW)	Litecoin's PoW consensus mechanism requires relatively low processing power	Litecoin prioritizes transactional efficiency through quicker block generation and lower-cost access to network participation, relative to Bitcoin
Monero (PoW)	Transactions on the Monero network are opaque by design, with most transaction details being unobservable to second and third parties	Monero is designed to be a truly anonymous payment network, with privacy and opacity features embedded in how the network processes and validates transactions. Monero's PoW consensus mechanism is designed to minimize the ability to pool ASIC[b] processing power
Ethereum (PoS)[c]	Developers proposed that the Ethereum network allows for relatively complex transaction processes on a permissionless blockchain by including a native programming layer. Initially reliant on PoW consensus, Ethereum is currently transitioning to PoS validation of network processes	Ethereum does not prioritize developing a lean peer-to-peer network to be used exclusively for transferring units of account, but rather emphasizes creating an environment for network users to program with application processing powered by network tokens, as well as a more flexible currency issuance rule
Tezos (PoS)	Tezos was founded to offer a network with governance features distinct from those that predominated among permissionless blockchains at the time. It was among the first to use PoS for block validation	Tezos uses a self-amendment process that avoids other blockchain protocols' forking. Network participants are chosen to validate blocks based upon their stake in the network
Cardano (PoS)	In Cardano's delegated staking protocol for achieving network consensus, network stakeholders delegate their stake to a validator pool in exchange for a proportion of the rewards for successful block validation	Cardano's consensus protocol was developed in response to weaknesses in existing PoS and delegated-PoS systems, but it retained these consensus mechanisms' benefits of lower processing time and energy intensity than PoW
Tether (permissioned)	A company-issued stable coin that claims to back the production of its coins by reserve assets	This type of token allows individuals to participate in decentralized-finance lending platforms and reduces the costs involved in transacting with other blockchain networks by ex-ante committing to a reserve that will back each unit of the stable coin

(Continued)

Table 1. (*Continued.*)

Cryptocurrency network (and consensus process)	Description	Differentiation
Ripple (permissioned)	A permissioned blockchain intended to function as a global (cross-border) payment network with only known and identifiable network participants permitted by Ripple ex-ante	Ripple is attempting to create a process for faster and easier international payments than the existing system while retaining the benefits of relatively centralized network governance

[a]Proof of work.
[b]Application-specific integrated circuit.
[c]Proof of stake.

terms of features, at least on paper. In practice, products usually compete in both quality and feature space, but to a different extent for each product pair. In each case, the question of whether to provide the same service at a higher quality or to provide a different service is more complex than it might seem. For a digital-currency network that is secured cryptographically and governed distributedly, is transactional anonymity a distinguishing feature or an essential characteristic? The Bitcoin white paper itself envisions highly opaque user identities (in line with the intended similarity to physical currency), although in practice identities have proven less than fully anonymous for many who wish to evade government scrutiny of their financial activity. In response to this lack of anonymity, the Monero network provides additional features.

At a more fundamental level, the distinctions among consensus mechanisms can be understood as a form of quality-based differentiation. However, for many network users, a permissioned consensus mechanism is no different from transacting through ordinary financial intermediaries, such that distinctions among consensus mechanisms can be ideological for many network participants and users. It is clear that the different networks are offering far more than one service of varying quality; instead, they offer competing sets of governance choices that distinguish one blockchain protocol from another. The lens of competitive governance can thus shed light on the characteristics that distinguish cryptocurrency networks from one another, for their development has displayed considerable differentiation in terms of consensus mechanisms, network transparency, block size, type of cryptographic hash puzzle, and many more network characteristics that provide margins of choice for protocol designers, and therefore, network users. The governance of a cryptocurrency thus depends not only on consensus building within a network, but also on how the many competing networks position themselves in response to their own governance needs.

Another reason for institutionalists to consider blockchain governance is competition's role in the evolution of institutional development. Markets for governance – specifically, well-aligned political property rights and competition in the provision of government services – contribute to more effective institutions (Salter and Piano, 2021). Through institutional competition in providing benefits to those governed to win their voluntary support, this process may yield more efficient institutions, all else equal. Crucially, though, this more expansive benefit to competitive governance depends on the governance choices of blockchain networks users and participants being sufficiently informed about the comparative benefits of different networks' institutional and protocol design choices, an assumption which is not entirely in line with the levels of uninformed speculative interest that these networks currently entertain (Alston, 2020). This problem of political (institutional) ignorance gives rise to a relatively small number of governance specialists, that ideally are constrained through the threat of exit, to make and enforce rules that are accessible to, and benefit, non-elites. The ongoing competitive development of blockchain network protocols and their governance provides a fertile field through which to examine this evolutionary institutional question.

6. Conclusion

Permissionless blockchains are a novel form of governance in the digital sphere. Fundamentally, the operation of a network is governed by the agreed-upon protocol, which the definition of and updates to can be understood as a form of dynamic constitutional choice. Despite the innovative way in which blockchain technology resolves certain challenges in distributed network governance, the networks are nonetheless complex human organizations that cannot foresee all future events that will require unique resolution. It makes the process of proposing, choosing, and adopting protocol changes central to understanding the constitutional-choice nature of the networks' internal governance processes. The ongoing political economy of protocol updates creates distinct interest groups of stakeholders subsidiary to the network itself, with developers and stakeholders of cryptocurrencies negotiating the specific institutional changes that define the future directions of the networks.

Since the networks are large and complex governance organizations, they face the usual politics of constitutional design and the requirement for rule changes. Competitive pressure and unanticipated events also force organizations to change. Despite their novelty in self-governance by protocols, blockchain networks require ongoing consensus among stakeholders as with most organizations. When the stakeholders cannot agree upon a shared vision for the network, an alternative platform may fork and compete with the incumbent, or new entrants will fill a competitive void in a rapidly developing asset class filled with institutional- and speculative-investor interest. We consider permissionless blockchains as internal constitutional collective-choice rules, and we view changes within the blockchain networks as resulting from competitive pressure interacting with these internal forces. Competition, therefore, constitutes a critical external force governing permissionless-cryptocurrency networks, for new software platforms often emerge when they see room for improvement. To explain the features (including performance, broadly defined) and changes in any given blockchain, one cannot only consider specific protocol-design choices made in isolation; it requires considering the polycentric set of governance forces we outline here.

Among the competitive forces likely to influence outcomes for cryptocurrency networks in coming years are digital units of account created by public governments, most commonly known as central bank digital currencies (CBDCs). While our comparative analysis is limited to private networks that produce blockchain-secured digital units of account, it is important to note that these networks' ability to competitively provide these features will increasingly be weighed against publicly produced digital currencies.

Power relations within blockchains (Berg, 2021) influence the extent to which the self-governing orders of blockchains are productive, equitable, and resilient.[29] The question of power relations within blockchains is likely to increase in significance as these networks' economic value and hence influence increases alongside their user bases and the digital exchange they facilitate, although competition should serve as a restraint unless network effects fully dominate.

The number of stakeholders in cryptocurrencies is relatively small today. For example, fewer than one hundred developers contribute to most of the code that runs today's networks. If the adoption of cryptocurrencies continues to rise, the governing body will very likely grow. How will the consensus arise? A discussion board is likely insufficient. Therefore, the processes to govern the system will be one of the most critical challenges in the years to come. Our analysis clarifies the sometimes-frustratingly complex set of polycentric governance forces that influences outcomes for any given permissionless cryptocurrency network in the hopes of improving the collective and competitive outcomes of these processes.

---

[29]Similar debates are playing out in internet governance more broadly (Benkler 2016) and in spectrum governance, where demands for access to spectrum are met in part by new technologies that enable sharing (Bustamante et al., 2020), much in the way blockchains were a partially liberating force from governments.

References

Aligica, P. D. and V. Tarko (2012), 'Polycentricity: From Polanyi to Ostrom, and Beyond', *Governance*, **25**(2): 237–262.

Allen, D. W. E., C. Berg, A.M. Lane, and J. Potts (2019), *Cryptodemocracy: How Blockchain Can Radically Expand Democratic Choice*, Landham, MD: Rowman & Littlefield.

Alston, E. (2020), 'Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets', *Case Western Journal of Law, Technology and the Internet*, **11**(5): 133–171.

Alston, E. (Forthcoming), 'Blockchain and the Law: Legality, Law-Like Characteristics, and Legal Applications', in J. Caton (ed), *Economics of Blockchain and Cryptocurrency: A Transaction Cost Revolution*, Northhampton: Edward Elgar.

Alston, E., L.J. Alston, B. Mueller, and T. Nonnenmacher (2018), *Institutional and Organizational Analysis: Concepts and Applications*, Cambridge University Press.

Alston, E., P. De Filippi, M. Mannan and N. Saul (2021), *Legitimizing Off-Chain Governance for Blockchain Networks*.

Alston, E., W. Law, I. Murtazashvili, M. Weiss (2021), 'Can Permissionless Blockchains Avoid Governance and the Law?', *Notre Dame Journal of Emerging Technologies*, **2**(1): 1–32.

Arruñada, B. (2018), 'Blockchain's Struggle to Deliver Impersonal Exchange', *Minnesota Journal of Law, Science and Technology*, **19**(1): 1955–1106.

Bartolucci, S., F. Caccioli, and P. Vivo (2020), 'A Percolation Model for the Emergence of the Bitcoin Lightning Network', *Scientific Reports*, **10**(1): 1–14.

Benkler, Y. (2016), 'Degrees of Freedom, Dimensions of Power', *Daedalus*, **145**(1): 18–32.

Berg, C. (2021), Rentseeking in blockchain governance: the awkward transition from market decisionmaking to non-market decisionmaking. *Available at SSRN*.

Berg, A. and C. Berg (2020), 'Exit, Voice, and Forking', *Cosmos + Taxis*, **8**(8–9): 76–89.

Boettke, P. J., A. W. Salter, and D. Smith (2021), *Money and the Rule of Law: Generality and Predictability in Monetary Institutions*, New York: Cambridge University Press.

Bonneau, J. (2015), "How long does it take for a Bitcoin transaction to be confirmed?" Coincenter. Retrieved from coincenter. org/education/crypto-regulation-faq/how-long-does-it-take-for-a-bitcoin-transaction-to-be-confirmed   published on November 3, 2015. Coincenter [online]. Available from: coincenter.org/education/crypto-regulation-faq/how-long-does-it-take-for-a-bitcoin-transaction-to-be-confirmed.

Bosu, A., A. Iqbal, R. Shahriyar, and P. Chakraborty (2019), 'Understanding the Motivations, Challenges and Needs of Blockchain Software Developers: A Survey', *Empirical Software Engineering*, **24**(4): 2636–2673.

Bustamante, P., M. M. Gomez, I. Murtazashvili, and M. Weiss (2020), 'Spectrum Anarchy: Why Self-Governance of the Radio spectrum Works Better Than we Think', *Journal of Institutional Economics*, **16**(6): 863–882.

Buterin, V. (2014), A next-generation smart contract and decentralized application platform. *white paper*. 3 (37).

Catalini, C. and J. S. Gans 2016, 'Some Simple Economics of the Blockchain', *NBER Working Paper 22952*.

Cowen, N. (2019), 'Markets for Rules: The Promise and Peril of Blockchain Distributed Governance', *Journal of Entrepreneurship and Public Policy*, **9**(2): 213–226.

Davidson, S., P. De Filippi, and J. Potts (2018), 'Blockchains and the Economic Institutions of Capitalism', *Journal of Institutional Economics*, **14**(4): 639–658.

De Filippi, P. and B. Loveluck (2016), 'The Invisible Politics of Bitcoin: Governance Crisis of A Decentralized Infrastructure', *Internet Policy Review*, **5**(4). https://doi.org/10.14763/2016.3.427.

De Filippi, P. and A. Wright (2018), *Blockchain and the law: The Rule of Code*, New York: Harvard University Press.

De Vries, A. (2018), 'Bitcoin's Growing Energy Problem', *Joule*, **2**(5): 801–805.

DuPont, Q. (2017), 'Experiments in Algorithmic Governance: A History and Ethnography of "The DAO," A Failed Decentralized Autonomous organization', in Malcolm Campbell-Verduyn (ed), *Bitcoin and Beyond*, London: Routledge. pp. 157–177.

Edmans, A., V. W. Fang and E. Zur (2013), 'The Effect of Liquidity on Governance', *The Review of Financial Studies*, **26**(6): 1443–1482.

Frolov, D. (2021), 'Blockchain and Institutional Complexity: An Extended Institutional Approach', *Journal of Institutional Economics*, **17**(1): 21–36. https://doi.org/10.1017/S1744137420000272.

Garriga, M., S. D. Palma, M. Arias, A. De Renzis, R. Pareschi, and D. A. Tamburri (2020), Blockchain and Cryptocurrencies: a Classification and Comparison of Architecture Drivers. *arXiv preprint arXiv:2007.12283*.

Halaburda, H. and M. Sarvary (2016), *Beyond Bitcoin*, New York: Palgrave Macmillan.

Halaburda, H., G. Haeringer, J. Gans and N. Gandal (2020), 'The Microeconomics of Cryptocurrencies', *NBER Working Paper 27477*, https://www.nber.org/papers/w27477.

Harris, C. (2018), 'Institutional solutions to free-riding in peer-to-peer networks: a case study of online pirate communities', *Journal of Institutional Economics*, **14**(5): 901–924.

Hirschman, A. O. (1970), *Exit, voice, and loyalty*, United Kingdom: Harvard University Press.

Howell, B. E. and P. H. Potgieter (2021), 'Uncertainty and Dispute Resolution for Blockchain and Smart Contract Institutions', *Journal of Institutional Economics*, **17**(4): 545–559.

Katz, M. L. and C. Shapiro (1985), 'Network Externalities, Competition, and Compatibility', *The American Economic Review*, **75**(3): 424–440.

King, R. S., S. Williams and D. Yanofsky (2013), By reading this article, you're mining bitcoins. Quartz [online]. Available from: https://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/.

Lee, B. E., D. J. Moroz and D. C. Parkes (2020), The Political Economy of Blockchain Governance. *Available at SSRN 3537314*.

Lin, J.-H., K. Primicerio, T. Squartini, C. Decker, and C. J. Tessone (2020), 'Lightning Network: A Second Path Towards Centralisation of the Bitcoin Economy', *New Journal of Physics*, **22**(8): 083022.

Li, X., P. Jiang, T. Chen, X. Luo, and Q. Wen (2020), 'A Survey on the Security of Blockchain Systems', *Future Generation Computer Systems*: 107: 841–853.

Lopp, J. (2018), 'Who Controls Bitcoin Core?' Blog post retrieved from, https://blog.lopp.net/who-controls-bitcoin-core-/ on September 21, 2020.

Luther, W. J. (2019), 'Getting off the Ground: The Case of Bitcoin', *Journal of Institutional Economics*, **15**(2): 189–205.

Luther, W. J. and S. Stein Smith (2020), 'Is Bitcoin A Decentralized Payment Mechanism?', *Journal of Institutional Economics*, **16**(4): 433–444.

Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system'. https://bitcoin.org/bitcoin.pdf.

Narayanan, A., J. Bonneau, E. Felten, A. Miller and S. Goldfeder (2016), *Bitcoin and Cryptocurrency Technologies: A Comprehensive introduction*, Princeton: Princeton University Press.

Newman, G., A. Wiggins, A. Crall, E. Graham, S. Newman, and K. Crowston (2012), 'The Future of Citizen Science: Emerging Technologies and Shifting Paradigms', *Frontiers in Ecology and the Environment*, **10**(6): 298–304.

Potts, J. (2018), 'Governing the Innovation Commons', *Journal of Institutional Economics*, **14**(6): 1025–1047.

Rajagopalan, S. (2018), 'Blockchain and Buchanan: Code as Constitution', in R. E. Wagner (ed.), *James M. Buchanan*, Cham, Switzerland: Springer. pp. 359–381.

Salter, A. W. and E. Piano (2021), 'The Fundamental Coase of Development: Property Rights Foundations of the Effective State', *Journal of Institutional Economics*, **17**(1): 37–52.

Salter, A. W. and V. Tarko (2017), 'Polycentric Banking and Macroeconomic Stability', *Business and Politics*, **19**(2): 365–395.

Sokolin, L. and M. Low (2018), 'Crypto Utopia.' Autonomous Research LLP. Retrieved from, https://www.lw.com/thoughtLeadership/crypto-utopia-autonomous-next on November 16, 2020.

Somin, I. (2020), *Free to Move: Foot Voting, Migration, and Political Freedom*, New York: Oxford University Press.

Weber, B. (2016), 'Bitcoin and the Legitimacy Crisis of Money', *Cambridge Journal of Economics*, **40**(1): 17–41.

Werbach, K. (2018), *The Blockchain and the New Architecture of Trust*, Cambridge: MIT Press.

White, L. H. (2015), 'The Market for Cryptocurrencies', *Cato Journal*, **35**(2): 383–402.

Williamson, O. E. (1996), *The Mechanisms of Governance*, New York: Oxford University Press.

Wright, A. and De Filippi, P. (2015), Decentralized blockchain technology and the rise of lex cryptographia. *Available at SSRN 2580664*.